UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/710,691	11/09/00	BOTS H	21055-701

TM02/0323

VINCENT K YIP
MCCUTCHEN DOYLE BROWN & ENERSEN LLP
THREE EMBARCADERO CENTER
SAN FRANCISCO CA 94111

EXAMINER	
BADERMAN, S	
ART UNIT	**PAPER NUMBER**
2184	5

DATE MAILED: 03/23/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
09/710,691	Bots et al.
Examiner	**Group Art Unit**
Scott T. Baderman	2184

☒ Responsive to communication(s) filed on *Nov 9, 2000* .

☐ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *1-11* is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *1-11* is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐approved ☐disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____ .

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____ .

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). *3*

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

Examiner: Scott T. Baderman

United States Department of Commerce

Patent and Trademark Office

Washington, D.C. 20231

DETAILED ACTION

Drawings

1. The drawings filed on November 9, 2000 have not yet been reviewed. Once this application is in condition for allowance, the drawings will be forwarded to the Official Draftsperson at that time.

Claim Objections

2. Claim 10 is objected to because of the following informalities: In line 3, "said first and second network addresses" should be "said first and second computer". Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless --

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 6 and 9 are rejected under 35 U.S.C. 102(a) as being anticipated by Shwed et al. (WO 97/00471).

As in claim 6, Shwed discloses a method for recovering (decrypting) an original data packet from a secure data packet sent between members of a virtual private network that comprises the steps of receiving the secure data packet, determining the packet manipulation rules for packets sent between members of the virtual private network, recovering the original data packet by manipulating the secure data packet by reversing the identified packet manipulation rules and forwarding the recovered data packet to its destination, wherein the secure data packet inherently contains information of a source address and a destination address of the secure data packet (Figure 16, page 4: lines 6-27, page 5: lines 5-30, page 13: lines 10-12, page 22: lines 28-30, page 25: line 16-page 26: line 13).

As in claim 9, Shwed discloses a system for securely exchanging data packets between members of a virtual private network group that comprises 1) a first computer (host 1) at a first site having a first network address, 2) a first router (inherently within the firewall 1) associated with the first site for routing data packets originating from the first computer over a public network, 3) a first virtual private network unit inherently disposed between the first router and the public network, wherein the first virtual private network identifies virtual private network group data traffic and secures the data traffic by manipulating the data traffic according to packet manipulation rules maintained by the first virtual private network unit, 4) a second router (inherently within firewall 2) associated with a second site for coupling the second site to the public network, 5) a second virtual private network unit inherently disposed between the second router and the public network for intercepting network traffic destined for the second site, wherein the second virtual private network unit detects virtual private network group traffic and recovers original packet data and 6) a second computer at the second site having a second network address for receiving the packet data, wherein the data packet inherently contains information of a source address and a destination address of the data packet (Figure 16, page 4: lines 6-27, page 13: lines 10-12, page 22: lines 28-30, page 25: line 16-page 26: line 13).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. (WO 97/00471) in view of Lidinsky et al. (4,897,874).

As in claim 1, Shwed discloses a method for sending a data packet from a first host to a second host through a virtual private network that comprises the steps of receiving the data packet en route to the second host, determining the packet manipulation rules for packets sent between the hosts through the virtual private network, forming a secure data packet by executing the packet manipulation rules on the data packet and forwarding the secure data packet to the second host through the virtual private network, wherein the secure data packet inherently contains information of a source address and a destination address of the secure data packet (Figures 5 and 16, Abstract, page 1: lines 27-29, page 2: lines 21-29, page 4: lines 6-27, page 5: lines 5-21, page 13: lines 10-12, page 14: lines 25-26, page 16: lines 3-26, page 22: lines 28-30, page 25: line 16-page 26: line 13). However, Shwed does not clearly disclose the step of determining that the data packet is being sent between *members* of the virtual private network.

Lidinsky discloses a method for protecting data transmitted in a virtual network from being accessed by unauthorized users outside of the network by determining that the data transmitted in the virtual network is being sent between members of the virtual network (Abstract, column 2: lines 3-6 and 56-63, column 3: lines 18-22).

It would have been obvious to a person skilled in the art at the time the invention was made to include the step of determining that a data packet is being sent between *members* of a virtual private network into the method taught by Shwed above. This would have been obvious because Lidinsky clearly teaches that "it is important that the privacy between different networks be carefully protected *by ensuring that no user not a member of a particular network has access to data of that network*" (column 3: lines 18-22), which would lead a person skilled in the art to include the step of determining that the data packet taught by Shwed above is sent between *members* of the virtual private network so that security is ensured like that taught by Lidinsky above.

As in claim 10, Shwed discloses the system above. However, Shwed does not clearly disclose a means for verifying that the data packet is being sent between *members* of the virtual private network. Lidinsky discloses a system for protecting data transmitted in a virtual network from being accessed by unauthorized users outside of the network by determining that the data transmitted in the virtual network is being sent between members of the virtual network (Abstract, column 2: lines 3-6 and 56-63, column 3: lines 18-22).

It would have been obvious to a person skilled in the art at the time the invention was made to include the means for verifying that a data packet is being sent between *members* of a virtual private network into the system taught by Shwed above. This would have been obvious because Lidinsky clearly teaches that "it is important that the privacy between different networks be carefully protected *by ensuring that no user not a member of a particular network has access to data of that network*" (column 3: lines 18-22), which would lead a person skilled in the art to include the means for verifying that the data packet taught by Shwed above is sent between *members* of the virtual private network so that security is ensured like that taught by Lidinsky above.

As in claim 11, Shwed and Lidinsky disclose the system above. Further, Shwed discloses forming a secure data packet by concealing (encrypting) the source and destination addresses of the data packet according to the manipulation rules (page 4: lines 10-12 and 25-27, page 5: lines 27-30).

7. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. in view of Lidinsky et al., as applied to claim 1 above, and further in view of Kirby et al. (5,828,846).

As in claim 2, Shwed and Lidinsky disclose the method above. However, neither clearly disclose a step of comparing source and destination addresses of a data packet to addresses stored in an address table in order to determine that the data packet is being sent between members of the virtual private network. Kirby discloses a method for controlling the passage of data packets via a virtual connection wherein source and destination addresses of the data packet are compared to addresses stored in an address table in order to determine whether passage of the data packet is valid (Figure 3, Abstract, column 1: lines 43-59, column 3: lines 4-11, column 4: lines 5-20).

It would have been obvious to a person skilled in the art at the time the invention was made to include a step of comparing source and destination addresses of a data packet to addresses stored in an address table in order to determine that the data packet is being sent between members of the virtual private network into the method taught by Shwed and Lidinsky above. This would have been obvious because Lidinsky clearly teaches that by determining that a data packet is being sent between *members* of a network, security is ensured that *no user not a member of a particular network has access to data of that network*, as was taught above, and Kirby clearly teaches that by comparing the source and destination addresses to a pre-stored address list in address table it can be determined whether the source and destination devices are valid to communicate with the data packet (column 4: lines 5-20), which is exactly what Lidinsky is trying to do. Based on the above teachings, a person skilled in the art would have been led to incorporate the teachings of Kirby into the method taught by Shwed and Lidinsky above in order

to determine that a data packet is being sent between *members* of a network since the method taught by Kirby will produce the results in which Lidinsky desires.

8. Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. in view of Lidinsky et al., as applied to claim 1 above, and further in view of Wesinger, Jr. et al. (5,898,830).

As in claim 3, Shwed and Lidinsky disclose the method above. Shwed further discloses methods that comprise algorithms, specifically encryption algorithms, to be utilized for data packets sent through the network (page 28: lines 17-26). However Shwed does not clearly disclose accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through the network. "Official Notice" is taken that lookup tables are well known in the art and are commonly used to maintain information in which a user or device can access. Wesinger discloses a method for controlling the passage of information through a network wherein channel processing can be performed, wherein the channel processing may include encryption, compression and authentication algorithms (Abstract, column 11: lines 35-60).

It would have been obvious to a person skilled in the art at the time the invention was made to include a step of accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through

the network into the method taught by Shwed and Lidinsky above. This would have been obvious because of the "Official Notice" statement made above and the teaching by Wesinger that channel processing is performed on data flowing through a communications channel to *enhance* some attribute of data, such as security, reproduction quality, etc. (column 11: lines 35-43), which would lead a person skilled in the art to incorporate the concept of channel processing into the method taught by Shwed and Lidinsky above since channel processing would actually provide an enhancement.

As in claim 4, Shwed, Lidinsky and Wesinger disclose the method above. Further, Shwed discloses forming a secure data packet by encrypting *at least* a payload portion of the data packet and providing authentication information for the data packet (page 4: lines 10-12, 25-27 and 31-page 5: lines 1-21).

As in claim 5, Shwed, Lidinsky and Wesinger disclose the method above. Further, Shwed discloses forming a secure data packet by concealing (encrypting) the source and destination addresses of the data packet according to the manipulation rules (page 4: lines 10-12 and 25-27, page 5: lines 27-30).

9. Claims 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shwed et al. in view of Wesinger, Jr. et al..

As in claim 7, Shwed discloses the method above. Shwed further discloses methods that comprise algorithms, specifically encryption algorithms, to be utilized for data packets sent through the network (page 28: lines 17-26). However Shwed does not clearly disclose accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through the network. "Official Notice" is taken that lookup tables are well known in the art and are commonly used to maintain information in which a user or device can access. Wesinger discloses a method for controlling the passage of information through a network wherein channel processing can be performed, wherein the channel processing may include encryption, compression and authentication algorithms (Abstract, column 11: lines 35-60).

It would have been obvious to a person skilled in the art at the time the invention was made to include a step of accessing a lookup table that maintains information identifying compression, encryption and authentication algorithms to be utilized for data packets sent through the network into the method taught by Shwed above. This would have been obvious because of the "Official Notice" statement made above and the teaching by Wesinger that channel processing is performed on data flowing through a communications channel to *enhance* some attribute of data, such as security, reproduction quality, etc. (column 11: lines 35-43), which would lead a person skilled in the art to incorporate the concept of channel processing into the method taught by Shwed above since channel processing would actually provide an enhancement.

As in claim 8, Shwed and Wesinger disclose the method above, wherein Shwed further discloses that the source and destination addresses are modified (encrypted, concealed), wherein once the packet is decrypted (recovered), inherently, the source and destination addresses will also be decrypted (recovered) (page 4: lines 6-9, page 25: lines 16-26).

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Scott T. Baderman whose telephone number is (703) 305-4644.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 308-9051, (for formal communications intended for entry)

Or:

(703) 305-3718 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Sixth Floor (Receptionist).

STB

March 22, 2001

Art Unit 2184